REMARKS

This amendment responds to the Office Action dated February 15, 2006 the examiner's interview on March 23, 2006. The examiner has previously provisionally withdrew certain claims (48-62, 78-89 and 153-160) from consideration because no generic claim was allowed. As stated later, applicant respectfully requests that the examiner find that independent claims (63, 90, 224) are patentable and reinstate claims 48-62, 78-89 and 153-160 provided applicant amends those claims in accordance with the corresponding independent claim.

In the Office Action on pages 2-9, the patent examiner rejected claims 63-77; 90-101 and 224-234 as being non-patentable in view of certain prior or pre-existing technology or art disclosed in the following references:

U.S. Patent No.5,960,080 to Fahlman
U.S. Patent No.5,581,682 to Anderson et al.
U.S. Patent No. 6,389,542 to Flyntz
U.S. Patent No. 6,598,161 to Kluttz et al.
U.S. Patent No. 5,036,315 to Gurley
FOLDOC (URL webpage)
Schneier (Applied Cryptography)

For the reasons set forth below, the current claims are patentably distinct from the cited references.

In summary, Fahlman '080, Andersen '682 and Flyntz '542 do not show, teach or suggest multiple extractions of security sensitive words INTO A RESPECTIVE plurality of memory stores for each security level (extract stores). Falman '080 does not disclose nor discuss multiple security level storage and retrieval. Anderson '682 describes storing all secure data in a single document (not multiple security storage locations, one for each security level) and Flyntz '542 does not discuss

STORING and RETRIEVING different security words from different extract or security memory locations.

Flyntz' 572 does not show, teach, or suggest the claimed (i) "filtering data input ... for said plurality of security levels and extracting ... for each of said security levels;" (claim 63) (ii) "storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store" (claim 63); (ii) "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores" (emphasis added)(claim 63); and (iv) as a result of permitting access "to respective ones of said extract stores", then permitting full or partial reconstruction of data "after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

Claims 90 and 224 have similar limitations, that is, extracting "for said plurality of security levels" and distributed storage of security sensitive data in a plurality of extract stores "corresponding to respective security levels." Claim 90. More significantly, Flyntz '542 (a) does not address storing different security words in corresponding different secured memories; and (b) does not require presentment of a plurality of predetermined security clearances "to obtain access to respective ones of said extract stores". Nowhere does Flyntz '542 discuss the storing of different security words in different memories, each for corresponding security level.

Flyntz '542 is principally interested in retrieving data but the retrieval of data always occurs with a double key system, the first key required is the user's smart card; and the second key required is a mechanical cam switch associated with a removable hard drive containing all complete versions of the secured documents for that security level. Only one memory store at a time is subject to access in Flyntz '542. As explained in detail later, if the security level on the user's smart card does not match the security level of the removable hard drive, the user is only permitted to retrieve and view unclassified data. Therefore, if the user's smart card has a high level of security rating (top secret, TS), and the hard drive is classified as secret (S), the user is not permitted access to the S data on the hard drive even though the user's security level is a higher TS rating compared with the security code on the hard drive S. Further, in every implementation of the Flyntz '542 patent, if this one to one correspondence (smart card security level must be equal hard drive security level) is NO, the user is only permitted access to the unclassified (U/C) data.

Flyntz '542 identifies three levels of data, unclassified (U/C), sensitive data (S) and classified (CL). These three (3) levels of secured data U/C, S and CL are identified in FIG. 1. A low level first security sub-system 51 (U/C hard drive 24), a second security sub-system 52 (S drive 15), and third level security level sub-system 53 (CL or drive 10) are illustrated. For the analysis herein, a similar nomenclature U/C, S and CL for low, medium and high secured data will be employed herein.

In every instance, Flyntz '542 requires that the smart card used by the user must match the security code of the hard drive (U/C; S; CL) and if not, the user is only permitted to see unclassified data U/C 24. An important feature of the Flyntz '542 system is that the data is on a removable hard drive. Col. 2, line 26 (herein "2/26"); 3/5; 3/31, 5/66; 7/30; 7/35; 7/38; 8/55; 9/41; 10/49; 11/33 ("if the nth memory device were detected by the (n-1)th sensor switch); 11/65; 12/4; 12/30; 12/40; 12/61; 13/15; 13/18; 13/37; 13/67. As explained in detail throughout Flyntz '542, the insertion of this removable hard drive (S or CL) closes a mechanical switch, such as a cam, and the closure of the S or CL drive cam, when matched to the S or CL security level on a smart card of a user, permits the user to access only the secured data on the inserted hard drive and not other data on any other hard drive. Flyntz '542 discusses the required matching between the security level on the user's smart card with the security level on the inserted hard drive memory (S or CL) at the following locations. Col. 2, line 40 (if no smart card, system loads from first security sub-system level U/C); Col. 3, lines 28-32 (when smart card security level matches inserted removable memory, "the computer operates only with the second security sub-system which is the only security sub-system connected to the computer power supply); 3/36; 4/2; 5/66; 6/53; 7/30 ("The installation of any other memory device does not close the first sensor switch S1 thereby preventing the activation of the second security sub-system 52 and maintaining the activation of the first security sub-system 51. It is the operation of the mechanically activated sensor switches that ensures that the correct memory device is installed and activated so that the store data at a given security level cannot be accessed or processed by devices and users at a different security level"); 8/54; 8/63; 9/55 ("process data at one security level during any given time"); 10/1 ("Each sub-system has unique physical characteristics that are utilized along with the user identification and authorization to ensure that the correct sub-system has been activated; the selection of a different security level must be done after logging out of the current level and allowing the operating system to turn the computer off so that the computer ram is cleared"); 10/34 (User access request for second level); 10/49 (If second memory device 15 were detected by first sensor switch as not being installed; default to U/C); 11/46; 11/64 ("There was also a mechanical interlock on the removable hard drives that automatically ensures that power is only applied to the drive, modem and NIC at the security level selected by the operator. The interlock essentially is a cam switch ... the location and configuration of the cam on the drive is keyed to the security level of the hard drive and is aligned to close only the switch in the drive bay that is set for that level"); 12/39 ("The basic principle for this computer system is the utilization of secured smart card identification and authentication of the user in combination with a mechanical interlock mechanism to control access to different security levels of a computer through the controlled application of power to the appropriate hard drives, modem, and NICs."); 12/59 ("The selection of higher level of security requires the entry and verification of the user identification and access rights coupled with the sensing of the correct removable hard [drive] for the security level selected through the action of the cam switches"); 11/66 ("The selection of a new security level can only be implemented after logging out of the operation system for the previous level and allowing the computer to power off").

The Flyntz '542 system powers only a single hard drive/security system at a time as discussed at 6/29; 6/53; 7/39; 8/40; 8/44; 8/63; 9/42; 9/58 ("process data at one security level during any given time"); 10/4 (log out required to access different security level systems); 10/43; 11/42; 11/65; 12/39 (control access to different security level systems through the controlled application of power); 12/66 (log out required to get to different security level); 13/9; 13/26; 16/6; and 16/34.

Flyntz '542 is exclusively dedicated toward the retrieval of data using a double key system -- the first key is the security code on the user's smart card and the second key is the cam sensing a certain security level hard drive in the removable memory bay. If the user's security code does not match the security level of the removable memory, the system defaults to the unclassified U/C memory. 2/40; 3/16; 6/29; 7/34; 8/21-27; 10/34-42; 11/24.

From the standpoint of analysis of the presently claimed invention, key portions of Flyntz '542 follow. "The second security sub-system has a removable memory device which is the only means for storing data at a second security level." 2/26. "The mechanically activated sensor switches, or cams, are key elements of the multi-level computer since they determine that the activation signal generated by the card reader should be transmitted to the electronically activated switches." 7/22. "Each sub-system can be coupled with the computer CPU, RAM and read only memory devices to comprise a complete computer system that can only access, store, and process data at one security level during any given time; only one sub-system can be activated at a given time with all others being electrically inactive." 9/53. "If the nth memory device were detected by the (n-1) th sensor switch S(n-1), the (n-1) th sensor switch would disable the transmission of the activation signal thus preventing the activation of the nth security sub-system and disabled the default activation of the first security sub-system until the smart card 30 is removed from the smart card reader." 11/33. "Each hard drive, modem, NIC, and LED are associated with a specific level of security access and or either powered ON or OFF depending on the security level selected by an authorized user. Access to the drives, modems, and NICs is based on the assigned access rights of the user as defined on their smart card 30 and the level of security access selected by the user from within their assigned security access rights. The hard drive, modem, NIC, and LED any given security level are directly connected such that power is either ON or OFF to all depending on the level of security access selected." 11/43. "There is also a mechanical interlock on the removable hard drives that automatically ensures that power is only applied to the drive, modem, and NIC at the security level selected by the operator." 11/64. "The location and configuration of the cam on the drive is keyed to the security level of the hard drive and is aligned to close only the switch in the drive bay that is set for that level." 12/4. "The basic principles of this computer system is a utilization of a secured smart card identification and authentication of the user in combination with a mechanical interlock mechanism to control access to different security levels of a computer through the controlled application of power through the appropriate hard drive." 12/39. "The selection of a higher level of security requires entry and verification of the user identification and access rights coupled with the sensing of the correct removable hard [drive] for the security level selected through the action of the cam switches." 12/59. "In addition, the selection of a new security level can only be implemented after logging out of the operating system for the previous level and allowing the computer to power off" 12/67. "The mechanical interlock also ensures that a mistake cannot be made by inserting a drive that is at a level that differs from what was selected and approved for the user via the smart card." 13/37.

Therefore, Flyntz '542 does not discuss in any manner the storage of security data at different "corresponding" security level storage sites. Flyntz deals with retrieval of data and isolation of power to only a single hard drive/security level. In direct contrast, the presently claimed invention specifically requires "storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store." Claim 63. Since Flyntz '542 requires a double key system where the user smart card security level must match the security level of the hard drive memory in the removable drive bay, all the data provided to that particular user must be found on that powered hard drive. Therefore, Flyntz '542 does not show, teach or suggest "storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store."

In addition, Flyntz '542 does not show, teach or suggest "filtering data input ... for said plurality of security levels and extracting ... for each of said security levels" nor "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores." Claim 63. It is absolutely clear that Flyntz '542 permits an authorized user to only access a single hard drive data store and not "respective ones of said extract stores" wherein each extract store corresponds "to respective security levels." Claim 63.

Anderson '682 does not show, teach or suggest storing extract data "in extract stores corresponding to respective security levels and said remainder data in said remainder store." Claim 63. Anderson '682 also does not show, teach or suggest "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores."

Anderson '682 shows that the security information is stored in a single document. For example, looking at the illustrations in Anderson '682, FIG. 2B shows a document and shows a data stream representing that document (see the bottom of the page, rectangular box with five segments including "begin page"). FIG. 3B shows an insert in the document "we should get a better map" which is not shown in the original document FIG. 2B and the added information "we should get a better map" is identified in the "object overlay" shown at the bottom of FIG. 3B after "begin page." FIG. 4 shows another insert in the original document "this needs a nice color picture." In the text of Anderson '682, the disclosure identifies that the document would include triplets (col. 3, line 65, herein "3/65") and theses triplets are shown in the table at 4/11 and include the length of triplet, the type of conditional overlay (normal, annotation or redaction) and the level of the overlay. "The level triplet is compared to one contained within the application being invoked and, if it is equal or lower than the application level, the overlay is processed. Otherwise, the overlay is not performed." 4/37. In applying the Anderson '682 system to a security item, the disclosure states:

> Returning to the decision block 4, if the overlay is a redaction, the system pursues to decision block 8. In decision block 8, the system examines the security level of the redaction and compares it to the security level of the user, which is already known to the system, if the redaction security level exceeds that of the user, the system determines that the user does not have ability to view the documents prior to redaction .

5/3.

Further, Anderson '682 specifically states "at this point, the system returns to block one in order to process any additional overlays that may be found in the current page of the document." Therefore, it is clear that the secure information or secure data in Anderson '682 is included in a single document and that secured data is stored with the document on the computer system. Therefore, Anderson '682 does not show, teach or suggest " storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder stores" which is a required step in claim 63, and also does not show, teach or suggest "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores." Claim 63.

The present invention requires multiple security levels, each having a sub-set of security sensitive words, extraction and storage for multiple security levels, a plurality of predetermined security clearances, a particular security clearance needed to access "respective ones of said extract stores" which extract stores are active "for respective ones of said plurality of security levels." Claim 63.

In the present invention, different security clearances permit access to different extract stores (each security level storage facility) in order to obtain the data and permit full or partial reconstruction "after presentment of respective ones of said plurality predetermined security clearances." Therefore, the present invention requires multiple extraction, each extraction for each security level, separate storage thereof, storage of the remainder or non-secured data ("storing ... said remainder data in said remainder store"), "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and, permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

Fahlman '080 does not show, teach or suggest a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of multiple levels, presentment of different security codes at each security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

In Fig. 1, step 111 of Fahlman "automatically" merges sensitive information into non-sensitive information. In FIG. 2, step 217, the Fahlman system again "automatically" merges secured data with un-secured data. Fahlman discusses merging secured data with unsecured data at col. 2, line 22, col. 2, line 34, and col. 2, line 49, and col. 2, line 54 and col. 2, line 40. Fahlman '080 discloses identifying security information and extracting that information and replacing it with place holders. Col. 2, line 37 and col. 3, line 47. "The sanitized message is then transmitted with a low level of security." Col. 3, line 54. The sensitive information is stripped from the original message and stored in a separate location or together with the sanitized message. Col. 3, line 64. A map showing the location of the security information is also stored with the secured information. Col. 3, line 63. "Then, in step 111, the sensitive terms received from the second path are merged with the sanitized message to create a final confidential message." Col. 4, line 1. The examiner should note that Fahlman does not discuss reconstruction or merger in the presence of any type of security clearance. In contrast, the present invention requires multiple security clearances, each unique to a security level. Fahlman also discusses: "Then, in step 217, the sensitive terms are automatically merged back into the serviced message to create a final message." Col. 5, line 27. No discussion of multi-level security clearance is noted. The same is true regarding merger of security information and non-secured information at col. 6, line 62.

Fahlman does not seem to store remainder or non-secure data in a separate remainder store location apart from secure data. Fahlman (1) identifies secret words, (2) replaces the words with placeholders, then (3) transmits the "sanitized message." Fig. 1, step 107, Fig. 2, step 209, col 2, line 19, col. 2, line 34, col. 2, line 49, col. 3, line 54 (transmission - no storage of non-secure data), col. 4, line 64 (transmission - no separate storage). Fahlman does discuss storing the sanitized message, that is, the non-secure data and the placeholders, but not separate storage of the remainder data. Col. 3, line 63, col. 4, line 47, col. 5, line 1. In the present invention, remainder, non-secret data is stored separately from secret data. See claim 63, "storing" step. Fahlman teaches away from this aspect of the present invention.

Fahlman does not discuss multiple security levels nor multiple storage sites at each security level. Since multiple security levels are not addressed in Fahlman, multiple security clearance codes to obtain "access" to the secured data levels is not discussed. Since Fahlman does not use any type of password or security clearance procedures, there is no "presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and, permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances." Claim 63.

A combination of Fahlman '080, Flyntz '542 and Anderson '682 results in a security system with a single, secure memory storage facility. No reference specifically discusses separate storage of non-secret, remainder data, separate storage of secure data in disparate secure data extract stores, and multiple access to multiple secure data stores. No reference shows, discusses or suggests multiple security levels and multiple stores for each level of security. Flyntz '542 stores secret data and non-secret data locally on a single, removable hard drive. To go from CL security level to S level, one must turn off the computer, remove the CL hard drive, insert the S hard drive, and re-start the computer with user smart card level S. Anderson '682 stores all data, secret and non-secret, in one document at one location. Fahlman extracts only a single level of data and transfers it separately from the non-secure data (data is transmitted by Fahlman, not stored "in a remainder store") but never discusses password control to access either type of data. It is respectfully submitted that it is improper to select disparate parts from each of these complicated systems and "cobble together" the claimed invention. There is no suggestion nor motivation to do so absent the disclosure of the present invention.

Each of the references, Fahlman '080, Flyntz '542 and Anderson '682 describe complete systems and there is no reason to add to or substitute portions of one disclosure with another. There is no evidence that a person of skill in the art would take certain aspects of one reference and add those features to another reference. For example, there is no reason to combine Flyntz' removable and separately powered S and CL hard drives with Anderson's singular document storage and reproduction system and/or Fahlman's secret data transmission system.

With respect to **Schneier's book (Applied Cryptography)**, Schneier does not show, teach or suggest multi-level extract stores nor "presenting a predetermined security clearance to obtain access to said extract store; and, permitting reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment thereof." Schneier discusses encryption and key destruction.

Kluttz '161 does not show, teach or suggest multi-level extract stores nor presenting a predetermined security clearance to obtain access to the multiple extract stores and permitting reconstruction of said data via said multiple extract stores and remainder data only in the presence of said predetermined security clearance after presentment thereof as required by the present invention. Kluttz '161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

The Kluttz '161disclosure does not show different levels of security for subsets of information. It discloses "dividing the document into at least a first portion having a first security level and a second portion having a second security level" and then encrypting these two levels differently. There is no different storage of different secure information with different password keys for each level, AND separate storage of remainder, non-secure data as per claim 63.

U.S. Patent No. 5,036,315 to Gurley does not cure the defects identified above. Gurley does not show, teach or suggest (a) filtering data; (b) utilizing multiple extract stores and a remainder store; (c) presenting a predetermined security clearance <u>to obtain access</u> to said multiple extract stores; and (d) permitting reconstruction of said data via said extract stores and remainder data only in the presence of said predetermined security clearance after presentment thereof. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

Kirshenbaum '298 does not show separate storage of secured data, separate and apart from unsecured data. Both secured and non-secured data is stored in a single database 14. Col. 3, lines 40-44; col. 5, lines 7-10 ("The data set is stored in a database ... the document comprises secure portion and non-secure portions"); col. 5, lines 36-37 ("to retrieve those secure and non-secure portions of the document and to send the retrieved portions of the document to the output device.").

Lamm '907 stores and has multiple copies of all secret-secured data about the consumer in three (3) different computers, to wit, consumer computer 12 (see legends FIG. 2, consumer computer 20, col. 5, line 48), billing - processor computer 26 (see col. 13, line 5) and enrollment server 21 (see col. 9, line 42). The three computers in Lamm '907 provide an integrated bill payment system which cannot be deconstructed into operable components. In contrast, the present invention extracts secured data, for multiple security levels, and then stores "said extracted data in extract stores corresponding to a respective security level and said remainder data in said remainder store." Lamm's process of storing secret data in three computers is completely different than the claimed system of storing secret data in multiple, "extract stores for respective ones of said plurality of security levels."

The examiner also cited, but did not apply, **U.S. Patent No. 5,903,646 to Rackman.** Rackman '646 discloses storing the original document, a redacted copy of the document, and sometimes a third version of the document in the same storage media. The various versions of these documents may be encrypted and the decryption keys distributed to select persons. See 4/18; 4/25 (two layers of confidentiality); 4/35 (the disk stores all versions of the document, both secure and unsecured versions); 6/30; 7/32; 7/52 (both redacted and un-redacted versions stored on same disc); 8/66; 10/3 (three versions, each with different levels of security, stored on same disc); 10/19; and 11/45.

The Manual of Patent Examining Procedures ("MPEP") explains that it is not obvious to modify a system with a plurality of sensors controlling a plurality of valves to create the inventive and patentable single sensor which controls a plurality of valves:

> In *In re Kotzab,* 217 F.3d 1365, 55 USPQ2d 1313 (Fed.Cir. 2000), the claims were drawn to an injection molding method using a single temperature sensor to control a plurality of flow control valves. The primary reference disclosed a multizone device having multiple sensors, each of which controlled an associated flow control valve, and also taught that one system may be used to control a number of valves. The court found that there was insufficient evidence to show that one system was the same as one sensor. While the control of multiple valves by a single sensor rather than by multiple sensors was a "technologically simple concept," there was no finding "as to the specific, understanding or principle within the knowledge of the skilled artisan" that would have provided the motivation to use a single sensor as the system to control more than one valve. 217 F.3d at 1371, 55 USPQ2d at 1318.

MPEP § 2143.01.

In the present invention, Applicant has developed a system designed to safeguard a plurality of security levels with specific dispersal and retrieval techniques. The single data storage systems of the prior art Fahlman '080, Andersen '682, Kluttz '161 and Flyntz '542 cannot be extended to the claimed multi-level security storage systems. Each of these references discloses single storage of security words. Flyntz '542 shows single storage because only one hard drive/security level system is powered ON at any one time.

> The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills,* 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990) (Claims were directed to an apparatus for producing an aerated cementitious composition by drawing air into the cementitious composition by driving the output pump at a capacity greater than the feed rate. The prior art reference taught that the feed means can be run at a variable speed, however the court found that this does not require that the output pump be run at the claimed speed so that air is drawn into the mixing chamber and is entrained in the ingredients during operation. Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.).

MPEP § 2143.01.

In the prior art cited herein, there is no suggestion of the desirability of multi-level secured data storage, extraction for each security level, and full or partial reconstruction using multiple extract stores. Further, the examiner's suggestion -- that Flyntz' S or CL hard drives, each with a unique cam-key and separate ON/OFF power control, be altered such that both the S and CL hard drives are active and are accessible to the user at the same time, -- "modifies" that reference to an unacceptable degree. "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)." MPEP § 2143.01. This change to Flyntz modifies the operation of the reference improperly. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)." MPEP § 2143.01.

Applicant respectfully requests that the examiner approve the patentability of claims 63-77; 90-101 and 224-234. Applicant respectfully requests that the examiner permit applicant to amend the other independent claims in elected invention Group II, that is, independent claims 48, 78 and 53, to conform to claim 63 (relative to multi-level security systems) since most of these claims 48, 78 and 153 (and dependent claims) become generic and patentable upon allowance of claim 63. After approval of the claims, Applicant will submit an appropriate terminal disclaimer.

[space left blank]

APPENDIX FOR CLAIMS

63. (Previously presented) A method for securing data in a computer network with one or more security sensitive words, characters or icons and a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, a first memory designated as a remainder store in said plurality of computers, and a corresponding plurality of memories in other ones of said plurality of computers designated as extract stores for respective ones of said plurality of security levels, comprising:

filtering data input from said data input computer for said plurality of security levels and extracting said security sensitive words, characters or icons for each of said security levels from said data to obtain extracted data for said security levels and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store;

presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and,

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of said predetermined security clearance after presentment of respective ones of said plurality of predetermined security clearances.

90. (Previously presented) A method for securing data in a computer network with one or more security sensitive words, characters or icons and a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, each of said plurality of computers having a memory therein, said plurality of computers including a first computer designated as a remainder store and a further plurality of computers designated as extract stores for respective ones of said plurality of security levels, comprising:

extracting said security sensitive words, characters or icons for said plurality of security levels from said data to obtain extracted data for respective security levels and remainder data;

storing said extracted data in extract stores corresponding to respective security levels and said remainder data in said remainder store;

presenting a plurality of predetermined security clearances to obtain access to respective ones of said extract stores; and,

permitting full or partial reconstruction of said data via said extracted data and remainder data only in the presence of respective ones of said predetermined security clearances after presentment thereof.

224. (Previously presented) An information processing system for securing data having one or more security sensitive words, characters or icons in a computer network, a plurality of security levels each with a respective security clearance, subsets of said security sensitive words, characters or icons being correlated with respective ones of said plurality of security levels, said computer network having a plurality of computers interconnected together, each of said plurality of computers having a memory therein, one of said plurality of computers designated as a data input computer, said plurality of computers including a first computer designated as a remainder computer store and a plurality of other computers designated as extract stores for respective ones of said plurality of security levels, the information processing system comprising:

a filter adapted to receive data input from said data input computer and to separate, from said data input, said security sensitive words, characters or icons into extracted data corresponding to respective ones of said plurality of security levels and remainder data;

a memory storage facility, coupled to said filter, for storing said extracted data in corresponding extract stores and said remainder data in said remainder store;

a security clearance control for each of said extract stores controlling access thereto only in the

presence of a predetermined respective one of a plurality of security clearances for each of said plurality of security levels; and

a compiler, coupled to said security control and said extract stores and said remainder store, for fully or partially reconstructing said data from said extracted data and said remainder data dependent upon access provided by respective ones of said plurality of security clearances.

Respectfully submitted,

By ______________________

Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Fort Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on March 27, 2006.

Robert C. Kain, Jr.
Reg. No. 30,648

\\TIGER\Data Share\RCK\CLIENTS\Redlich\Patents\6851-02-amdt-3d-032706.wpd